

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

ai sensi del GDPR 2016/679 e normativa nazionale in vigore

**COMUNE DI CHERASCO
AMMINISTRAZIONE PUBBLICA**

TITOLARE

BOGETTI CLAUDIO

SEDE

**COMUNE DI CHERASCO
CHERASCO**

Data revisione: 15/07/2025

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla

protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

OBBLIGO DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

- a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

CRITERI DA CONSIDERARE PER OBBLIGO DPIA

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

REVISIONE

Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità.

ALGORITMO VALUTAZIONE

1° STEP: identificazione dei trattamenti

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

2° STEP: valutazione del rischio e individuazione criteri per DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento (**C**). Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

$$LR = P \times C$$

LR = livello di rischio

P = probabilità di accadimento

C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

P r o b a b i l i t à	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
Conseguenze						

Entità Rischio	Valori di riferimento
Accettabile	$(1 \leq LR \leq 3)$
Medio - basso	$(4 \leq LR \leq 6)$
Rilevante	$(8 \leq LR \leq 12)$
Alto	$(15 \leq LR \leq 25)$

Si ricava, così, per ogni attività di trattamento un **Livello di Rischio** (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico

4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

3 STEP: DPIA - valutazione del rischio normalizzato

Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevedono due o più criteri di obbligo DPIA.

Nel caso in cui, quindi, l'indice di rischio si colloca nel range $15 \div 25$, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.

La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

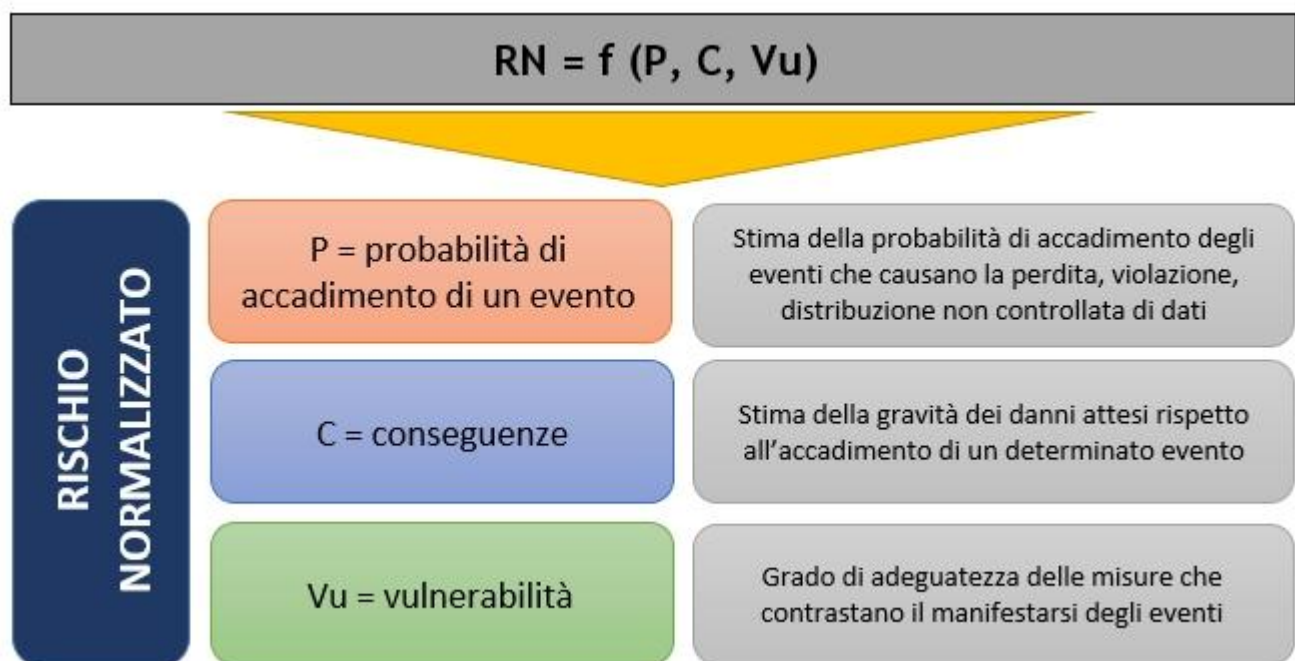
Il rischio viene calcolato in funzione dei 3 fattori seguenti:

$$RN = f(P, C, Vu)$$

Dove:

P = probabilità

C = conseguenze generate dall'evento



V = vulnerabilità rispetto al grado di adeguatezza delle misure

In prima battuta viene ricavato il rischio intrinseco R_i come prodotto della probabilità P e delle conseguenze C , in base agli indici numerici assegnati ad entrambi i fattori.

Alla probabilità P è associato un indice numerico rappresentato nella seguente tabella:

Probabilità	
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

Alle conseguenze (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

P R O B A B I L I T À	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
CONSEGUENZE					

RISCHIO INTRINSECO	
Ri = P x C	Valori di riferimento
Molto basso	$(1 \leq Ri \leq 2)$
Basso	$(3 \leq Ri \leq 4)$
Rilevante	$(6 \leq Ri \leq 9)$
Elevato	$(12 \leq Ri \leq 16)$

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.

Di seguito la suddivisione delle aree di pericolo con i rischi generati.

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	• Perdita • Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	• Perdita • Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla **Vulnerabilità (Vu)** è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		Valore
1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

V u	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	Valori di riferimento
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Elevato	$12 \leq RN \leq 16$

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia **ALTA**, il Titolare attiva l'iter di consultazione del Garante.

RISULTATI DPIA

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

Elenco attività sottoposte a DPIA

- REGISTRO FORNITORI - REGISTRO FORNITORI - Titolare del trattamento
- REGISTRO UTENTI - REGISTRO UTENTI - Titolare del trattamento
- DIPENDENTI E COLLABORATORI - DIPENDENTI E COLLABORATORI - Titolare del trattamento

REGISTRO FORNITORI - REGISTRO FORNITORI - Titolare del trattamento

Struttura	• Amministrazione • Sede legale • Sede operativa
Personale coinvolto	
Titolare del trattamento	BOGETTI CLAUDIO
Persone autorizzate	Dott. BOGETTI CLAUDIO, c.f. BGTCLD65C10B111G • Conservazione • Consultazione • Utilizzo
	Avv. GATTO CARLA MARIA, c.f. GTTCLM60A63F809K • Blocco • Cancellazione • Comunicazione • Conservazione • Consultazione • Elaborazione • Modifica • Organizzazione • Raccolta • Raffronto • Utilizzo
	Arch. ABRATE LUCIANO • Cancellazione • Conservazione • Consultazione • Elaborazione • Modifica • Utilizzo
	Rag. RAIMONDO VITTORIO • Cancellazione • Conservazione • Consultazione • Elaborazione

- Modifica
- Utilizzo

Sig.ra DOGLIANI PATRIZIA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig.ra BONINO MICHELINA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig.ra RADAELLI GIOVANNA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Dott. DOGLIANI FRANCESCO MARIO

- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Dott.ssa FERRERO VALENTINA

- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig.ra LONGO MONICA

- Conservazione
- Elaborazione
- Modifica

Ragioniera TARICCO CRISTINA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Geom. SICCA MAURO

- Cancellazione
- Conservazione
- Consultazione

- Elaborazione
- Modifica
- Utilizzo

Geom. CANNATARO GIUSEPPINO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig.ra ASSELLE DANIELA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Ing. MARENGO MASSIMO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Arch. DOTTA DOMENICO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Geom. BORRA GIOVANNI

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig. BOSSOLASCO MARCO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Geom. BRESCIA PIERO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica

- Utilizzo

Dott.ssa MOLINO OLIMPIA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Dott. PERANO LIVIO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

MARTINENGO GERMANO GIACOMO STEFANO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig. BAUDISSONE MIRKO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Arch. CANNATARO DANIELE

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Arch. CAREGLIO MAURO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Arch. CIRAVEGNA GIULIO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

	Arch. GILLIO FILIPPO • Cancellazione • Conservazione • Consultazione • Elaborazione • Modifica • Utilizzo Arch. MARENCO MAURIZIO • Cancellazione • Conservazione • Consultazione • Elaborazione • Modifica • Utilizzo Dott. SANTAGATA GABRIEL • Cancellazione • Conservazione • Consultazione • Elaborazione • Modifica • Utilizzo Arch. TARICCO CRISTINA • Cancellazione • Conservazione • Consultazione • Elaborazione • Modifica • Utilizzo Dott.ssa ZEFI ANDI • Cancellazione • Conservazione • Consultazione • Elaborazione • Modifica • Utilizzo
Partners - Responsabili esterni	AREA S.r.l., p.iva 02971560046 • Conservazione • Elaborazione
Altro	

Processo di trattamento	
Descrizione	REGISTRO DEI FORNITORI
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Legge
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Legge
Finalità del trattamento	Albo fornitori Adempimento di obblighi fiscali o contabili Adempimento di obblighi di legge connessi a rapporti commerciali Adempimenti agli obblighi di legge Approvvigionamento

	Emissione fatture in formato elettronico Gestione dei fornitori (contratti, ordini, arrivi, fatture) ASSISTENZA HARDWARE E SOFTWARE Prevenzione del contagio da COVID - 19 Attività di consulenza Attività di volontariato Autorizzazioni, concessioni, permessi, licenze e nullaosta Attività sportive Attività turistiche e ricreative Gestione contabile o di tesoreria Gestione del contenzioso (contratti, ordini, arrivi, fatture) Servizi assicurativi (responsabilità civile, ramo vita, sanità e calamità)
Tipo di dati personali	Dati di comunicazione elettronica Dati relativi all'attività economica e commerciale Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)
Categorie di interessati	Agenti e Rappresentanti Artigiani Commercianti Consulenti e liberi professionisti, anche in forma associata Creditori Enti Fornitori Imprenditori e piccoli imprenditori Industrie Iscritti in albi ed elenchi Lavoratori Autonomi Lavoratori atipici Membri di organismo di controllo PMI (Piccole e Medie Imprese) Potenziali fornitori Revisori Soggetti o organismi pubblici
Categorie di destinatari	Agenzia delle Entrate Camere di commercio, industria, artigianato ed agricoltura Consulenti e liberi professionisti anche in forma associata Altre amministrazioni pubbliche Associazioni e fondazioni Associazioni ed enti locali Enti pubblici economici Gestori posta elettronica Medico competente R.S.P.P. Fornitori di servizi informatici Imprese di assicurazione Organizzazioni di volontariato Persone autorizzate Piattaforme di elaborazione
Informativa	Non necessaria
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	All'occorrenza
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario per lo svolgimento delle attività tipiche di una Amministrazione Comunale.
Trasferimento dati (paesi terzi)	No

Autorizzazione del Garante	Non presente
-----------------------------------	--------------

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Pacchetto Office JAVA SISCOM ACROBAT ADOBE SISCOM : FINANZIARIA AMMINISTRATIVA IMPOSTE E TASSE E DEMOGRAFICI GISMASTER: PROTOCOLLO SUAP E SUE TIME & WORK: REGISTRAZIONE PRESENZE DEL PERSONALE
Strutture informatiche di archiviazione	
SERVER LINUX	Struttura interna
Sede di riferimento	COMUNE DI CHERASCO
Personale con diritti di accesso	TECNOLOGIE DIGITALI S.r.l., p.iva 03034820047
Software utilizzati	- MICROSOFT OFFICE - SISCOM: FINANZIARIA AMMINISTRATIVA IMPOSTE E TASSE E DEMOGRAFICI - GISMASTER: PROTOCOLLO SUAP E SUE - TIME & WORK: REGISTRAZIONE PRESENZE DEL PERSONALE - ADOBE ACROBAT
Strutture informatiche di backup	
SERVER LINUX	Struttura interna
Sede di riferimento	COMUNE DI CHERASCO
Frequenza di backup	1 Giorni
Tempo di storicizzazione	1 Giorni
Personale con diritti di accesso	TECNOLOGIE DIGITALI S.r.l., p.iva 03034820047
Note	
Software utilizzati	- MICROSOFT OFFICE - SISCOM: FINANZIARIA AMMINISTRATIVA IMPOSTE E TASSE E DEMOGRAFICI - GISMASTER: PROTOCOLLO SUAP E SUE - TIME & WORK: REGISTRAZIONE PRESENZE DEL PERSONALE - ADOBE ACROBAT

VALUTAZIONE DEL LIVELLO DI RISCHIO			
RISCHIO	PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Accesso dati non autorizzato	Poco probabile	Trascurabili	Accettabile
Distruzione non autorizzata	Poco probabile	Trascurabili	Accettabile
Divulgazione non autorizzata	Poco probabile	Trascurabili	Accettabile
Modifica non autorizzata	Improbabile	Trascurabili	Accettabile
Perdita	Poco probabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati - Configurata la modalità di blocco automatico quando ci si allontani dalla postazione di lavoro - Dispositivi antincendio - E' applicata una gestione della password degli utenti - E' applicata una procedura per la gestione degli accessi - E' eseguita la DPIA

- E' presente una politica per la sicurezza e la protezione dei dati
- E' prevista la distruzione dei supporti rimovibili non utilizzati
- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati
- Esistono procedure per l'individuazione del custode delle password
- GESTIONE DEL SERVER
- I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali contatti stretti di un lavoratore risultato positivo al COVID-19.
- I dati sono trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19.
- I documenti vengono firmati digitalmente
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Il dato non viene registrato
- Il dato relativo alla temperatura corporea non viene registrato.
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- In caso di isolamento momentaneo dovuto al superamento della soglia di temperatura viene garantita la riservatezza delle informazioni limitandone la diffusione.
- Le credenziali sono disattivate in caso di perdita della qualità
- Le credenziali sono disattivate se inutilizzate per sei mesi
- Le password sono costituite da almeno otto caratteri alfanumerici
- Le password sono modificate al primo utilizzo
- Le password sono modificate ogni 3 mesi
- Le procedure sono riesaminate con cadenza predefinita
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Registrazione e deregistrazione degli utenti
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti
- Sono applicate regole per la gestione delle password.
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono eseguiti gli aggiornamenti di sicurezza del sistema operativo
- Sono gestiti i back up
- Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili
- Sono stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- Vengono registrati e conservati i Log file
- Viene effettuata la registrazione ed il controllo degli accessi
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SICUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate

	• PERDITA DEI DATI	
Configurata la modalità di blocco automatico quando ci si allontani dalla postazione di lavoro	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Dispositivi antincendio	• Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
E' applicata una gestione della password degli utenti	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
E' applicata una procedura per la gestione degli accessi	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione,	Adeguate

	ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
E' eseguita la DPIA	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
E' presente una politica per la sicurezza e la protezione dei dati	• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
E' prevista la distruzione dei supporti rimovibili non utilizzati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate

Esistono procedure per l'individuazione del custode delle password	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
GESTIONE DEL SERVER	• Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Eventi naturali (Terremoti) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • PERSONAL COMPUTER • PERSONAL COMPUTER - SERVER • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Terremoti	Adeguate
I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali contatti stretti di un lavoratore risultato positivo al COVID-19.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
I dati sono trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

	• ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
I documenti vengono firmati digitalmente	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Il dato non viene registrato	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Il dato relativo alla temperatura corporea non viene registrato.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
In caso di isolamento momentaneo dovuto al superamento della soglia di temperatura viene garantita la riservatezza	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

delle informazioni limitandone la diffusione.	• ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
Le credenziali sono disattivate in caso di perdita della qualità	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Le credenziali sono disattivate se inutilizzate per sei mesi	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Le password sono costituite da almeno otto caratteri alfanumerici	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Le password sono modificate al primo utilizzo	• Compromissione informazioni (intercettazioni, rivelazione	Adeguate

	informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
Le password sono modificate ogni 3 mesi	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Le procedure sono riesaminate con cadenza predefinita	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione,	Adeguate

elettroniche e cartacee	ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
Registrazione e deregistrazione degli utenti	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sistemi di allarme e di sorveglianza anti-intrusione	• Agenti fisici (incendio, allagamento, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono applicate regole per la gestione delle password.	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso	Adeguate

	non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono eseguiti gli aggiornamenti di sicurezza del sistema operativo	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono gestiti i back up	• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER	Adeguate

	• PERSONAL COMPUTER • Terremoti • Eventi naturali (Terremoti)	
Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono stabiliti programmi di formazione e sensibilizzazione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono utilizzati software antivirus e anti intrusione	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Vengono registrati e conservati i Log file	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Viene effettuata la	• Compromissione informazioni	Adeguate

registrazione ed il controllo degli accessi	(intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Viene eseguita una regolare formazione del personale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO

Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso

VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO
ARCHIVIO INFORMATICO

RISCHI		
• Accesso dati non autorizzato • Divulgazione non autorizzata • Modifica non autorizzata • Distruzione non autorizzata • Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
PERSONAL COMPUTER - SERVER		
RISCHI		
• Accesso dati non autorizzato • Divulgazione non autorizzata • Modifica non autorizzata • Distruzione non autorizzata • Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
PERSONAL COMPUTER		
RISCHI		
• Accesso dati non autorizzato • Divulgazione non autorizzata • Modifica non autorizzata • Distruzione non autorizzata • Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso

VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Terremoti		
RISCHI		
Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Eventi naturali (Terremoti)		
RISCHI		
Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

A valle della DPIA l'attività risulta a rischio **Molto basso**

REGISTRO UTENTI - REGISTRO UTENTI - Titolare del trattamento

Struttura	- Sede legale - Sede operativa
Personale coinvolto	
Titolare del trattamento	BOGETTI CLAUDIO

Persone autorizzate

Dott. BOGETTI CLAUDIO, c.f. BGTCLD65C10B111G

- Conservazione
- Consultazione
- Utilizzo

Avv. GATTO CARLA MARIA, c.f. GTTCLM60A63F809K

- Blocco
- Cancellazione
- Comunicazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Raccolta
- Raffronto
- Utilizzo
- UTILIZZO

Arch. ABRATE LUCIANO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig.ra ASSELLE DANIELA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig. BAUDISSONE MIRKO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig.ra BONINO MICHELINA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Geom. BORRA GIOVANNI

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig. BOSSOLASCO MARCO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Geom. BRESCIA PIERO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Geom. CANNATARO GIUSEPPINO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Dott.ssa CHIAVAZZA SARA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Dott. DOGLIANI FRANCESCO MARIO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig.ra DOGLIANI PATRIZIA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Dott.ssa FERRERO VALENTINA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Dott.ssa INNOCENTI LICIA VITTORIA

- Cancellazione

- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig.ra LONGO MONICA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Ing. MARENGO MASSIMO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

MARTINENGO GERMANO GIACOMO STEFANO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Dott.ssa MOLINO OLIMPIA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig.ra PANERO MARIA TERESA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Dott. PERANO LIVIO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig. PREGLIASCO SERGIO

- Cancellazione
- Conservazione
- Consultazione

- Elaborazione
- Modifica
- Utilizzo

Sig.ra RADAELLI GIOVANNA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Rag. RAIMONDO VITTORIO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Geom. SICCA MAURO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Ragioniera TARICCO CRISTINA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig. TARICCO FEDERICO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Sig.ra TEALDI CATERINA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Geom. VAIRA GIAMPIERO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica

- Utilizzo

Arch. CANNATARO DANIELE

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Arch. CAREGLIO MAURO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Arch. CIRAVEGNA GIULIO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Arch. GILLIO FILIPPO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Arch. MARENCO MAURIZIO

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Arch. TARICCO CRISTINA

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

Dott. SANTAGATA GABRIEL

- Cancellazione
- Conservazione
- Consultazione
- Elaborazione
- Modifica
- Utilizzo

	Dott.ssa ZEFI ANDI • Cancellazione • Conservazione • Consultazione • Elaborazione • Modifica • Utilizzo
Partners - Responsabili esterni	TECNOLOGIE DIGITALI S.r.l., p.iva 03034820047 • Conservazione MAGGIOLI S.p.A., p.iva 02066400405 • Conservazione • Elaborazione SISCOM SPA, p.iva 01778000040 • Conservazione • Elaborazione • Modifica AREA S.r.l., p.iva 02971560046 • Consultazione • Elaborazione • Modifica TECNICAL DESIN S.r.l., p.iva 00595270042 • Conservazione • Consultazione
Altro	

Processo di trattamento	
Descrizione	Attività di gestione delle relazioni con i UTENTI / CLIENTI
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Legge
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Legge
Finalità del trattamento	Servizio di accettazione dei pagamenti Elaborazione, stampa, imbustamento e spedizione delle fatture Adempimento di obblighi fiscali o contabili Adempimenti agli obblighi di legge Servizi sociali ed assistenza Gestione Data Protection Prevenzione del contagio da COVID - 19 Gestione del contenzioso
Tipo di dati personali	Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali) Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)
Categorie di interessati	Cittadini Utenti
Categorie di destinatari	Persone autorizzate

	Consulenti e liberi professionisti anche in forma associata Autorità sanitarie Enti previdenziali ed assistenziali Organismi per i collegi professionali Servizi di giustizia e di polizia Servizi pubblici Uffici giudiziari Studi legali
Informativa	Non necessaria
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	All'occorrenza
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario per lo svolgimento delle attività tipiche di una Amministrazione Comunale.
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Pacchetto Office ACROBAT ADOBE PAGHE@PA SISCOM
Strutture informatiche di archiviazione	
SERVER LINUX	Struttura interna
Sede di riferimento	COMUNE DI CHERASCO
Personale con diritti di accesso	TECNOLOGIE DIGITALI S.r.l., p.iva 03034820047
Software utilizzati	- MICROSOFT OFFICE - SISCOM: FINANZIARIA AMMINISTRATIVA IMPOSTE E TASSE E DEMOGRAFICI - GISMASTER: PROTOCOLLO SUAP E SUE - TIME & WORK: REGISTRAZIONE PRESENZE DEL PERSONALE - ADOBE ACROBAT
Strutture informatiche di backup	
SERVER LINUX	Struttura interna
Sede di riferimento	COMUNE DI CHERASCO
Frequenza di backup	1 Giorni
Tempo di storicizzazione	1 1
Personale con diritti di accesso	TECNOLOGIE DIGITALI S.r.l., p.iva 03034820047
Note	
Software utilizzati	- MICROSOFT OFFICE - SISCOM: FINANZIARIA AMMINISTRATIVA IMPOSTE E TASSE E DEMOGRAFICI - GISMASTER: PROTOCOLLO SUAP E SUE - TIME & WORK: REGISTRAZIONE PRESENZE DEL PERSONALE - ADOBE ACROBAT

VALUTAZIONE DEL LIVELLO DI RISCHIO			
RISCHIO	PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Accesso dati non autorizzato	Poco probabile	Trascurabili	Accettabile
Distruzione non autorizzata	Poco probabile	Marginali	Medio-basso
Divulgazione non	Poco probabile	Trascurabili	Accettabile

autorizzata			
Modifica non autorizzata	Poco probabile	Trascurabili	Accettabile
Perdita	Poco probabile	Marginali	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Configurata la modalità di blocco automatico quando ci si allontani dalla postazione di lavoro
- Dispositivi antincendio
- E' applicata una gestione della password degli utenti
- E' eseguita la DPIA
- E' presente una politica per la sicurezza e la protezione dei dati
- E' prevista la distruzione dei supporti rimovibili non utilizzati
- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati
- Esistono procedure per l'individuazione del custode delle password
- GESTIONE DEL SERVER
- I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali contatti stretti di un lavoratore risultato positivo al COVID-19.
- I dati sono trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19.
- I documenti vengono firmati digitalmente
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Il dato non viene registrato
- Il dato relativo alla temperatura corporea non viene registrato.
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- In caso di isolamento momentaneo dovuto al superamento della soglia di temperatura viene garantita la riservatezza delle informazioni limitandone la diffusione.
- Le credenziali sono disattivate in caso di perdita della qualità
- Le credenziali sono disattivate se inutilizzate per sei mesi
- Le password sono costituite da almeno otto caratteri alfanumerici
- Le password sono modificate al primo utilizzo
- Le password sono modificate ogni 3 mesi
- Le procedure sono riesaminate con cadenza predefinita
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Registrazione e deregistrazione degli utenti
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti
- Sono applicate regole per la gestione delle password.
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono eseguiti gli aggiornamenti di sicurezza del sistema operativo
- Sono gestiti i back up
- Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili
- Sono stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- Vengono registrati e conservati i Log file
- Viene effettuata la registrazione ed il controllo degli accessi
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SICUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER • PERDITA DEI DATI	Adeguate
Configurata la modalità di blocco automatico quando ci si allontani dalla postazione di lavoro	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Dispositivi antincendio	• Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
E' applicata una gestione della password degli utenti	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate

E' eseguita la DPIA	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
E' presente una politica per la sicurezza e la protezione dei dati	• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
E' prevista la distruzione dei supporti rimovibili non utilizzati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Esistono procedure per l'individuazione del custode delle password	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

	• ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
GESTIONE DEL SERVER	• Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Eventi naturali (Terremoti) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • PERSONAL COMPUTER • PERSONAL COMPUTER - SERVER • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Terremoti	Adeguate
I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali contatti stretti di un lavoratore risultato positivo al COVID-19.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
I dati sono trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate

I documenti vengono firmati digitalmente	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Il dato non viene registrato	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Il dato relativo alla temperatura corporea non viene registrato.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
In caso di isolamento momentaneo dovuto al superamento della soglia di temperatura viene garantita la riservatezza delle informazioni limitandone la diffusione.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate

Le credenziali sono disattivate in caso di perdita della qualità	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Le credenziali sono disattivate se inutilizzate per sei mesi	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Le password sono costituite da almeno otto caratteri alfanumerici	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Le password sono modificate al primo utilizzo	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso	Adeguate

	non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
Le password sono modificate ogni 3 mesi	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Le procedure sono riesaminate con cadenza predefinita	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate

Registrazione e deregistrazione degli utenti	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sistemi di allarme e di sorveglianza anti-intrusione	• Agenti fisici (incendio, allagamento, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono applicate regole per la gestione delle password.	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate

Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono eseguiti gli aggiornamenti di sicurezza del sistema operativo	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono gestiti i back up	• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER • Terremoti • Eventi naturali (Terremoti)	Adeguate
Sono presenti istruzioni per	• Azioni non autorizzate (Errori	Adeguate

la custodia e l'uso dei supporti rimovibili	volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
Sono stabiliti programmi di formazione e sensibilizzazione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono utilizzati software antivirus e anti intrusione	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Vengono registrati e conservati i Log file	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Viene effettuata la registrazione ed il controllo degli accessi	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori	Adeguate

	volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Viene eseguita una regolare formazione del personale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata		

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN

Molto basso	0,25	Molto basso
-------------	------	-------------

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
ARCHIVIO INFORMATICO		
RISCHI		
• Accesso dati non autorizzato • Divulgazione non autorizzata • Modifica non autorizzata • Distruzione non autorizzata		

Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
PERSONAL COMPUTER - SERVER		
RISCHI		
- Accesso dati non autorizzato - Divulgazione non autorizzata - Modifica non autorizzata - Distruzione non autorizzata - Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
PERSONAL COMPUTER		
RISCHI		
- Accesso dati non autorizzato - Divulgazione non autorizzata - Modifica non autorizzata - Distruzione non autorizzata - Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN

Molto basso	0,25	Molto basso
-------------	------	-------------

PERICOLO		
Terremoti		
RISCHI		
Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Eventi naturali (Terremoti)		
RISCHI		
Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

A valle della DPIA l'attività risulta a rischio **Molto basso**

DIPENDENTI E COLLABORATORI - DIPENDENTI E COLLABORATORI - Titolare del trattamento

Struttura	- Sede legale - Sede operativa
Personale coinvolto	
Titolare del trattamento	BOGETTI CLAUDIO
Persone autorizzate	Avv. GATTO CARLA MARIA, c.f. GTTCLM60A63F809K - Blocco - Cancellazione - Comunicazione

	• Conservazione • Consultazione • Elaborazione • Modifica • Raccolta • Raffronto • Utilizzo Dott. BOGETTI CLAUDIO, c.f. BGTCLD65C10B111G • Consultazione Dott. DOGLIANI FRANCESCO MARIO • Cancellazione • Conservazione • Consultazione • Elaborazione • Utilizzo Dott.ssa FERRERO VALENTINA • Cancellazione • Conservazione • Consultazione • Elaborazione • Utilizzo Sig.ra LONGO MONICA • Cancellazione • Conservazione • Consultazione • Elaborazione • Utilizzo Geom. SICCA MAURO • Cancellazione • Conservazione • Consultazione • Elaborazione • Utilizzo Sig.ra BONINO MICHELINA • Cancellazione • Conservazione • Consultazione • Elaborazione • Utilizzo Ragioniera TARICCO CRISTINA • Cancellazione • Conservazione • Consultazione • Elaborazione • Utilizzo
Partners - Responsabili esterni	TECNOLOGIE DIGITALI S.r.l., p.iva 03034820047 • Conservazione ALMA SPA, p.iva 00572290047 • Cancellazione

	• Conservazione • Elaborazione • Modifica SISCOM SPA, p.iva 01778000040 • Conservazione • Elaborazione • Modifica VIGLIETTA & COMPANY SAS, p.iva 01945470043 • Conservazione • Elaborazione • Modifica Ing. TOVOLI DAVIDE MARIO LILLO, c.f. TVLDDM70A17F205Q • Consultazione
Altro	

Processo di trattamento	
Descrizione	GESTIONE DIPENDENTI E COLLABORATORI
Fonte dei dati personali	Raccolti direttamente Forniti da terzi
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Legge Implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. 1, n.7, lett. d) del DPCM 11 marzo 2020 Contratto Consenso
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Legge Implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. 1, n.7, lett. d) del DPCM 11 marzo 2020 Contratto Consenso
Finalità del trattamento	Adempimenti agli obblighi di legge Prevenzione del contagio da COVID - 19 Gestione del personale Reclutamento, selezione, valutazione e monitoraggio del personale: concorsi interni Trattamento giuridico ed economico del personale
Tipo di dati personali	Dati relativi alla famiglia e a situazioni personali Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare) Abitudini di vita o di consumo (viaggi, spostamenti, preferenze o esigenze alimentari) Adesione a sindacati o organizzazioni a carattere sindacale Amministrazione personale Anagrafica delle risorse umane aziendali Beni, proprietà, possessi (proprietà, possessi e locazioni; beni e servizi forniti o ottenuti) Codice Fiscale e altri numeri di identificazione personale Convinzioni filosofiche o di altro genere, adesioni ad organizzazioni a carattere filosofico Convinzioni religiose, adesioni ad organizzazioni a carattere religioso Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. Dati di comunicazione elettronica Dati di geolocalizzazione

	Dati finanziari Dati genetici per l'identificazione univoca di una persona Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Dati identificativi dell'orientamento sessuale Dati personali protetti dal segreto professionale Dati personali relativi a condanne penali e reati Dati relativi a malattie professionali Dati relativi ad infortuni Dati relativi alla prestazione lavorativa Dati relativi all'attività economica e commerciale Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali) Dati sulla salute Indirizzi IP di provenienza Informazioni per la fatturazione e dati di pagamento (ragione sociale, P.IVA, coordinate bancarie, codice fiscale, indirizzo) Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae) Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) Opinioni politiche Origini razziali o etniche Particolari (sensibili) Personalì Anagrafe dei Cittadini
Categorie di interessati	Agenti e Rappresentanti Amministratori Artigiani Candidati per eventuale rapporto di lavoro Cittadini Collaboratori Commercianti Consulenti e liberi professionisti, anche in forma associata Controparti Creditori Detenuti o sottoposti a misure di sicurezza o di prevenzione Dipendenti Docenti Enti Familiari dell'interessato Fornitori Imprenditori e piccoli imprenditori Industrie Iscritti in albi ed elenchi Lavoratori Lavoratori atipici Lavoratori Autonomi Membri di organismo di amministrazione Membri di organismo di controllo Personale pubblico dirigenziale e magistrati PMI (Piccole e Medie Imprese) Potenziati fornitori R.S.P.P. Revisori Soggetti o organismi pubblici

	Utenti
Categorie di destinatari	Agenzia delle Entrate Altre amministrazioni pubbliche Associazioni di imprenditori e di imprese Associazioni e fondazioni Associazioni ed enti locali Autorità di vigilanza e controllo Autorità sanitarie Camere di commercio, industria, artigianato ed agricoltura Consulenti e liberi professionisti anche in forma associata Dipendenti Enti locali Enti pubblici economici Enti pubblici non economici Federazioni Sportive Fornitori di servizi informatici Gestori posta elettronica Imprese Medico competente Organismi paritetici in materia di lavoro Organizzazioni di volontariato Organizzazioni sindacali e patronati Organizzazioni sportive Persone autorizzate Piattaforme di elaborazione R.S.P.P. Rappresentante dei lavoratori per la sicurezza Responsabili interni Servizi pubblici Soggetti che svolgono attività di archiviazione della documentazione Studi legali Interessati
Informativa	Non necessaria
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	All'occorrenza
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario per lo svolgimento delle attività tipiche di una Amministrazione Comunale.
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Pacchetto Office
Strutture informatiche di archiviazione	
SERVER LINUX	Struttura interna
Sede di riferimento	COMUNE DI CHERASCO
Personale con diritti di accesso	TECNOLOGIE DIGITALI S.r.l., p.iva 03034820047
Software utilizzati	- MICROSOFT OFFICE - SISCOM: FINANZIARIA AMMINISTRATIVA IMPOSTE E TASSE E DEMOGRAFICI - GISMASTER: PROTOCOLLO SUAP E SUE - TIME & WORK: REGISTRAZIONE PRESENZE DEL PERSONALE - ADOBE ACROBAT
Strutture informatiche di backup	
SERVER LINUX	Struttura interna

Sede di riferimento	COMUNE DI CHERASCO
Frequenza di backup	1 1
Tempo di storicizzazione	1 1
Personale con diritti di accesso	TECNOLOGIE DIGITALI S.r.l., p.iva 03034820047
Note	
Software utilizzati	- MICROSOFT OFFICE - SISCOM: FINANZIARIA AMMINISTRATIVA IMPOSTE E TASSE E DEMOGRAFICI - GISMASTER: PROTOCOLLO SUAP E SUE - TIME & WORK: REGISTRAZIONE PRESENZE DEL PERSONALE - ADOBE ACROBAT

VALUTAZIONE DEL LIVELLO DI RISCHIO

PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Poco probabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Configurata la modalità di blocco automatico quando ci si allontani dalla postazione di lavoro
- Dispositivi antincendio
- E' applicata una gestione della password degli utenti
- E' eseguita la DPIA
- E' presente una politica per la sicurezza e la protezione dei dati
- E' prevista la distruzione dei supporti rimovibili non utilizzati
- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati
- Esistono procedure per l'individuazione del custode delle password
- GESTIONE DEL SERVER
- I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali contatti stretti di un lavoratore risultato positivo al COVID-19.
- I dati sono trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19.
- I documenti vengono firmati digitalmente
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Il dato non viene registrato
- Il dato relativo alla temperatura corporea non viene registrato.
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- In caso di isolamento momentaneo dovuto al superamento della soglia di temperatura viene garantita la riservatezza delle informazioni limitandone la diffusione.
- Le credenziali sono disattivate in caso di perdita della qualità
- Le credenziali sono disattivate se inutilizzate per sei mesi
- Le password sono costituite da almeno otto caratteri alfanumerici
- Le password sono modificate al primo utilizzo
- Le password sono modificate ogni 3 mesi
- Le procedure sono riesaminate con cadenza predefinita
- L'impianto elettrico è certificato ed a norma
- Organizzare all'interno della propria abitazione una postazione di lavoro dedicata. con appositi device, analogamente a quella lavorativa.
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Registrazione e deregistrazione degli utenti
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti

- Sono applicate regole per la gestione delle password.
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono eseguiti gli aggiornamenti di sicurezza del sistema operativo
- Sono gestiti i back up
- Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili
- Sono stabiliti programmi di formazione e sensibilizzazione
- Sono utilizzati software antivirus e anti intrusione
- Vengono registrati e conservati i Log file
- Viene effettuata la registrazione ed il controllo degli accessi
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SICUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER • PERDITA DEI DATI	Adeguate
Configurata la modalità di blocco automatico quando ci si allontani dalla postazione di lavoro	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Dispositivi antincendio	• Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
E' applicata una gestione della password degli utenti	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate

	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
E' eseguita la DPIA	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
E' presente una politica per la sicurezza e la protezione dei dati	• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
E' prevista la distruzione dei supporti rimovibili non utilizzati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate

Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Esistono procedure per l'individuazione del custode delle password	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
GESTIONE DEL SERVER	• Agenti fisici (incendio, allagamento, attacchi esterni) • ARCHIVIO INFORMATICO • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Eventi naturali (Terremoti) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • PERSONAL COMPUTER • PERSONAL COMPUTER - SERVER • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Terremoti	Adeguate
I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER	Adeguate

degli eventuali contatti stretti di un lavoratore risultato positivo al COVID-19.	PERSONAL COMPUTER	
I dati sono trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19.	- Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) - ARCHIVIO INFORMATICO - PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER	Adeguate
I documenti vengono firmati digitalmente	- Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) - ARCHIVIO INFORMATICO - PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER	Adeguate
I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	- Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) - ARCHIVIO INFORMATICO - PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER	Adeguate
Il dato non viene registrato	Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Il dato relativo alla temperatura corporea non viene registrato.	- Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) - ARCHIVIO INFORMATICO - PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER	Adeguate
Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	- Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) - Agenti fisici (incendio, allagamento, attacchi esterni) - ARCHIVIO INFORMATICO	Adeguate

	- PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER	
In caso di isolamento momentaneo dovuto al superamento della soglia di temperatura viene garantita la riservatezza delle informazioni limitandone la diffusione.	- Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) - ARCHIVIO INFORMATICO - PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER	Adeguate
Le credenziali sono disattivate in caso di perdita della qualità	- Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) - Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) - Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) - ARCHIVIO INFORMATICO - PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER	Adeguate
Le credenziali sono disattivate se inutilizzate per sei mesi	- Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) - Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) - ARCHIVIO INFORMATICO - PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER	Adeguate
Le password sono costituite da almeno otto caratteri alfanumerici	- Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) - Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

	ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
Le password sono modificate al primo utilizzo	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Le password sono modificate ogni 3 mesi	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Le procedure sono riesaminate con cadenza predefinita	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	Adeguate

	• ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
Organizzare all'interno della propria abitazione una postazione di lavoro dedicata. con appositi device, analogamente a quella lavorativa.	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Registrazione e deregistrazione degli utenti	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sistemi di allarme e di sorveglianza anti-intrusione	• Agenti fisici (incendio, allagamento, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	Adeguate

	• ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono applicate regole per la gestione delle password.	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER	Adeguate

	PERSONAL COMPUTER	
Sono eseguiti gli aggiornamenti di sicurezza del sistema operativo	- Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) - ARCHIVIO INFORMATICO - PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER	Adeguate
Sono gestiti i back up	- Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) - Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) - Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) - Agenti fisici (incendio, allagamento, attacchi esterni) - ARCHIVIO INFORMATICO - PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER - Terremoti - Eventi naturali (Terremoti)	Adeguate
Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili	- Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) - Agenti fisici (incendio, allagamento, attacchi esterni) - ARCHIVIO INFORMATICO - PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER	Adeguate
Sono stabiliti programmi di formazione e sensibilizzazione	- Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) - ARCHIVIO INFORMATICO - PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER	Adeguate
Sono utilizzati software antivirus e anti intrusione	Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in	Adeguate

	messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	
Vengono registrati e conservati i Log file	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Viene effettuata la registrazione ed il controllo degli accessi	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • ARCHIVIO INFORMATICO • PERSONAL COMPUTER - SERVER • PERSONAL COMPUTER	Adeguate
Viene eseguita una regolare formazione del personale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • ARCHIVIO INFORMATICO	Adeguate

	- PERSONAL COMPUTER - SERVER - PERSONAL COMPUTER	
--	---	--

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
- Perdita - Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
- Perdita - Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato		

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

		RN
Molto basso	0,25	Molto basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
ARCHIVIO INFORMATICO		
RISCHI		
• Accesso dati non autorizzato • Divulgazione non autorizzata • Modifica non autorizzata • Distruzione non autorizzata • Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
PERSONAL COMPUTER - SERVER		
RISCHI		
• Accesso dati non autorizzato • Divulgazione non autorizzata • Modifica non autorizzata • Distruzione non autorizzata		

Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO <i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
PERSONAL COMPUTER		
RISCHI		
- Accesso dati non autorizzato - Divulgazione non autorizzata - Modifica non autorizzata - Distruzione non autorizzata - Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO <i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Terremoti		
RISCHI		
Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO <i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO

Eventi naturali (Terremoti)		
RISCHI		
Perdita		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO <i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

A valle della DPIA l'attività risulta a rischio **Molto basso**